

BUCKET FILE COPY ORIGINAL

June 25, 2008

Ms. Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street SW
Suite TW-A325
Washington, DC 20554

FILED/ACCEPTED

JUN 25 2008

Federal Communications Commission
Office of the Secretary

Re: San Juan Cable, LLC - Annual CPNI Compliance Certification
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), enclosed, please find an original and four copies of the annual CPNI compliance certification of San Juan Cable, LLC d/b/a OneLink Communications ("OneLink"). This certification covers the period from December 8, 2007, when the Commission's CPNI rules became applicable to voice-over-Internet-Protocol ("VOIP") providers such as OneLink,¹ through the date of the certification.

Very truly yours,

Jorge Hernandez w. permission
Jorge Hernandez *AMB*
Vice President and CFO

OneLink Communications
1 Calle Manuel Camuñas
Urb. Tres Monjitas
San Juan, PR 00918-1485
Phone: (787) 766-0909
Fax: (787) 641-9859
Email: jorge.hernandez@onelinkpr.com

¹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115; WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007); *FCC Announces Effective Date of Amended Customer Proprietary Network Information (CPNI) Rules*, DA 07-4915, Public Notice (December 6, 2007).

0 + f

JUN 25 2008

Federal Communications Commission
Office of the Secretary**CERTIFICATE OF COMPLIANCE WITH PROTECTION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION RULES**

Jorge Hernandez signs this Certificate of Compliance (this "Certificate"), in accordance with 47 C.F.R. § 64.2009(e), on behalf of San Juan Cable, LLC d/b/a Onelink Communications (the "Company"). This Certificate addresses the requirement of 47 C.F.R. § 64.2009(e) that the Company provide both a certificate of compliance and a "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 C.F.R. § 64.2001 - 64.2009.

On behalf of the Company, I certify as follows:

1. I am the Vice President and Chief Financial Officer of the Company. My business address is 1 Calle Manuel Camunas, San Juan, PR 00918-1485.
2. I have personal knowledge of the facts stated in this Certificate. I am responsible for overseeing the Company's compliance with the Federal Communications Commission's ("FCC") rules relating to the protection of customer proprietary network information ("CPNI"), as defined in 47 U.S.C § 222(h)(1).
3. Company personnel are not permitted to make any decisions regarding use of CPNI without first consulting with a supervisor from the Customer Operations Department. The Company's disciplinary policies and procedures are applied to personnel who make unauthorized use or other disclosure of CPNI.
4. The Company does not disclose CPNI to customers (or anyone else) over the telephone; if customers want to access CPNI, they must visit the Company in person and present valid photo identification. In addition, the Company requires password authentication for customer-initiated access to customers' online accounts. These passwords, as well as the procedure used to authenticate a caller's identity if such caller has forgotten his or her password, effectively protect customers' CPNI from "data brokers."
5. The Company's policy is not to disclose CPNI to third parties, including joint venture partners and affiliates.
6. Company personnel, prior to making any use of CPNI, must first consult with a supervisor regarding the lawfulness of using the CPNI in the manner contemplated. In deciding whether the contemplated use of the CPNI is proper, management considers one or more of the following: the Company's own compliance policies, the applicable FCC regulations, the FCC's Compliance Guide, and, if necessary, legal counsel. The Company's sales personnel and Customer Operations personnel must obtain supervisory approval regarding any proposed use of CPNI.
7. As encouraged by the FCC, the Company has implemented several additional CPNI protective measures. All of the Company's computer systems and databases containing CPNI are encrypted to prevent unauthorized access.
8. The Company is cognizant of the dangers of "pretexting," and therefore, in the event that the Company detects attempts by so-called "data brokers" to use pretexting against it or otherwise to access CPNI, the Company will conduct an internal investigation to determine

the source of the problem and the most appropriate resolution, which may involve reporting such pretexting activity to the FCC or other applicable governmental authorities

9. The Company has not received any complaints with respect to misuse, unauthorized disclosure, or other problems with respect to its handling or protection of CPNI since the FCC's CPNI rules became applicable to interconnected VoIP service providers on December 8, 2007.

This certification is respectfully submitted on this 23rd day of June, 2008.



Jorge Hernandez
Vice President and Chief Financial Officer